

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

1.1. Область применения программы:

Рабочая программа производственной практики составлена в соответствии с требованиями ФГОС СПО по специальности 10.02.01 Организация и технология защиты информации утвержден приказом Министерством образования и науки Российской Федерации от 28 июля 2014г. №805 зарегистрирован Министерством юстиции 21 августа 2014г. №33750, укрупненная группа 10.00.00 Информационная безопасность, утверждена приказом Минобрнауки России от 29 октября 2013г. №1199, единого тарифно-квалификационного справочника работ и профессий рабочих (ЕТКС).

1.2. Цели и задачи производственной практики

Целью производственной практики является:

закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин общепрофессионального цикла и дисциплин профессиональных модулей.

Основными задачами производственной практики являются:

- формирование у обучающихся общих и профессиональных компетенций;
- приобретение навыков работы с информационными системами, используемыми на предприятии, в организации или учреждении;
- приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника;
- изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации;
- формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения;
- получение навыков реализации различных алгоритмов и механизмов защиты информации;
- адаптация обучающихся к конкретным условиям деятельности предприятий различных организационно-правовых форм.

1.3. Место производственной практики в структуре ООП СПО

а) В соответствии с ФГОС производственная практика является обязательной, она представляет собой вид занятий, непосредственно ориентированных на профессионально-практическую подготовку обучающихся.

б) Программа производственной практики является частью ООП в соответствии с ФГОС по специальности СПО 10.02.01 Организация и технология защиты информации в части освоения основных видов профессиональной деятельности:

ПМ.01. Участие в планировании и организации работ по обеспечению защиты объекта;

ПМ.02 Организация и технология работы с конфиденциальными документами;

ПМ. 03 Программно-аппаратные и технические средства защиты информации;

ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих.

в) Производственная практика направлена на закрепление, расширение, углубление и систематизацию знаний, полученных при изучении специальных дисциплин, на основе изучения деятельности конкретного предприятия, приобретение практического опыта и профессионального мышления.

1.4. Компетенции обучающегося, формируемые в результате прохождения практики:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ОК 10. Применять математический аппарат для решения профессиональных задач.

ОК 11. Оценивать значимость документов, применяемых в профессиональной деятельности.

ОК 12. Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.

ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.

ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте.

ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации.

ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности.

ПК 1.5. Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации.

ПК 1.6. Обеспечивать технику безопасности при проведении организационно-технических мероприятий.

ПК 1.7. Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите.

ПК 1.8. Проводить контроль соблюдения персоналом требований режима защиты информации.

ПК 1.9. Участвовать в оценке качества защиты объекта.

ПК 2.1. Участвовать в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации.

ПК 2.2. Участвовать в организации и обеспечивать технологию ведения делопроизводства с учетом конфиденциальности информации.

ПК 2.3. Организовывать документооборот, в том числе электронный, с учетом конфиденциальности информации.

ПК 2.4. Организовывать архивное хранение конфиденциальных документов.

ПК 2.5. Оформлять документацию по оперативному управлению средствами защиты информации и персоналом.

ПК 2.6. Вести учет работ и объектов, подлежащих защите.

ПК 2.7. Подготавливать отчетную документацию, связанную с эксплуатацией средств контроля и защиты информации.

ПК 2.8. Документировать ход и результаты служебного расследования.

ПК 2.9. Использовать нормативные правовые акты, нормативно-методические документы по защите информации.

ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах.

ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.

ПК 3.3. Проводить регламентные работы и фиксировать отказы средств защиты.

ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.

По итогам прохождения производственной практики обучающийся **должен:**

ПМ.01. Участие в планировании и организации работ по обеспечению защиты объекта иметь практический опыт:

- использования физических средств защиты объекта;
- применение физических средств контроля доступа на объект;
- ведение текущей работы исполнителей с конфиденциальной информацией;
- *ведения учета и оформления бумажных и машинных носителей конфиденциальной информации;*
- *работы с информационными системами электронного документооборота.*

уметь:

- организовывать охрану персонала, территорий, зданий, помещений и продукции организаций;
- пользоваться аппаратурой систем контроля доступа;
- выделять зоны доступа по типу и степени конфиденциальности работ;
- определять порядок организации и проведения рабочих совещаний;
- использовать методы защиты информации в рекламной и выставочной деятельности;
- использовать критерии подбора и расстановки сотрудников подразделений защиты информации;
- организовывать работу с персоналом, имеющим доступ к конфиденциальной информации;
- проводить инструктаж персонала по организации работы с конфиденциальной информацией;
- контролировать соблюдение персоналом требований защиты информации;
- *использовать в профессиональной деятельности нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;*
- *разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации;*
- *документировать ход и результаты служебного расследования;*
- *определять состав документируемой конфиденциальной информации;*
- *подготавливать, издавать и учитывать конфиденциальные документы;*
- *составлять номенклатуру конфиденциальных дел;*
- *формировать и оформлять конфиденциальные дела;*
- *организовывать и вести конфиденциальное делопроизводство, в том числе с использованием вычислительной техники;*
- *использовать системы электронного документооборота.*

знать:

- виды и способы охраны объекта;
- особенности охраны персонала организации;
- основные направления и методы организации режима и охраны объекта;
- разрешительную систему доступа к конфиденциальной информации;
- принципы действия аппаратуры систем контроля доступа;
- принципы построения и функционирования биометрических систем безопасности;
- требования и особенности оборудования режимных помещений;
- требования и порядок реализации режимных мер в ходе подготовки и проведения совещаний по конфиденциальным вопросам и переговоров;
- требования режима защиты информации при приеме в организации посетителей;
- организацию работы при осуществлении международного сотрудничества;

- требования режима защиты информации в процессе рекламной деятельности;
- требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати;
- задачи, функции и структуру подразделений защиты информации;
- принципы, методы и технологию управления подразделений защиты информации;
- методы проверки персонала по защите информации;
- процедуру служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией;
- *основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;*
- *правовые основы защиты конфиденциальной информации по видам тайны;*
- *порядок получения права предприятия на ведение работ, связанных с конфиденциальной информацией;*
- *правовые основы деятельности подразделений защиты информации;*
- *правовую основу допуска и доступа персонала к защищаемым сведениям;*
- *правовое регулирование взаимоотношений администрации и персонала в области защиты информации;*
- *систему правовой ответственности за утечку информации и утрату носителей информации;*
- *правовые нормы в области защиты интеллектуальной собственности;*
- *порядок отнесения информации к разряду конфиденциальной информации;*
- *порядок разработки, учета, хранения, размножения и уничтожения конфиденциальных документов;*
- *организацию конфиденциального документооборота;*
- *технологию работы с конфиденциальными документами;*
- *организацию электронного документооборота*

ПМ.02 Организация и технология работы с конфиденциальными документами;

иметь практический опыт:

- ведения учета и оформления бумажных и машинных носителей конфиденциальной информации;
- работы с информационными системами электронного документооборота;

уметь:

- использовать в профессиональной деятельности нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации;
- документировать ход и результаты служебного расследования;
- определять состав документируемой конфиденциальной информации;
- подготавливать, издавать и учитывать конфиденциальные документы;
- составлять номенклатуру конфиденциальных дел;
- формировать и оформлять конфиденциальные дела;
- организовывать и вести конфиденциальное делопроизводство, в том числе с использованием вычислительной техники;

- использовать системы электронного документооборота;
- *проводить информационные обследования, выявлять значимые угрозы, анализировать и оценивать риски, применять различные защитные механизмы;*
- *разрабатывать нормативно-методические и организационно-распорядительные документы, необходимые для реализации выбранных технологий защиты;*
- *определение подходов к оценке характеристик и выбору необходимых программно-аппаратных и программных средств защиты информационных ресурсов, основы поиска и использования оперативной информации об угрозах и средствах защиты, другой актуальной информации по безопасности автоматизированных систем;*
- *контролировать и анализировать эффективность применения конкретных мер и средств защиты информации;*
- *грамотно выстроить на предприятии политику безопасности.*
- *логически обрабатывать информацию, имеющую значение для реализации правовых норм в соответствующих сферах профессиональной деятельности;*
- *готовить документы о передаче прав на информационные объекты, отражающие информационно-правовой режим и порядок доступа к информации.*

знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- правовые основы защиты конфиденциальной информации по видам тайны;
- порядок лицензирования деятельности по технической защите конфиденциальной информации;
- правовые основы деятельности подразделений защиты информации;
- правовую основу допуска и доступа персонала к защищаемым сведениям;
- правовое регулирование взаимоотношений администрации и персонала в области защиты информации;
- систему правовой ответственности за утечку информации и утрату носителей информации;
- правовые нормы в области защиты интеллектуальной собственности;
- порядок отнесения информации к разряду конфиденциальной информации;
- порядок разработки, учета, хранения, размножения и уничтожения конфиденциальных документов;
- организацию конфиденциального документооборота;
- технологию работы с конфиденциальными документами;
- организацию электронного документооборота;
- *правовые вопросы защиты информации;*
- *теории построения защищенных систем;*
- *организацию работы подразделений информационной безопасности;*
- *основы построения комплексных систем защиты, обеспечивающих рациональное распределение функций и эффективное взаимодействие по вопросам защиты информации сотрудников всех структурных подразделений организации;*
- *эксплуатационные характеристики основных средств защиты информации (средства предотвращения несанкционированного доступа, криптографическая защита, межсетевые экраны, средства анализа защищенности и обнаружения атак);*
- *основы поиска и использования оперативной информации о новых уязвимостях в системном и прикладном программном обеспечении.*

- пути совершенствования правовой основы информационного пространства России;
- проблемы международного сотрудничества в правовом регулировании и развитии глобального информационного пространства

**ПМ. 03 Программно-аппаратные и технические средства защиты информации;
иметь практический опыт:**

- участия в эксплуатации систем и средств защиты информации защищаемых объектов;
- применения технических средств защиты информации;
- выявления возможных угроз информационной безопасности объектов защиты;

уметь:

- работать с техническими средствами защиты информации;
- работать с защищенными автоматизированными системами;
- передавать информацию по защищенным каналам связи;
- фиксировать отказы в работе средств вычислительной техники;

знать:

- виды, источники и носители защищаемой информации;
- источники опасных сигналов;
- структуру, классификацию и основные характеристики технических каналов утечки информации;
- классификацию технических разведок и методы противодействия им;
- методы и средства технической защиты информации;
- методы скрытия информации;
- программно-аппаратные средства защиты информации;
- структуру подсистемы безопасности операционных систем и выполняемые ею функции;
- средства защиты в вычислительных сетях;
- средства обеспечения защиты информации в системах управления базами данных;
- критерии защищенности компьютерных систем;
- методики проверки защищенности объектов информатизации на соответствие требованиям нормативных правовых актов.

ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих.

Код профессии: 16199. Оператор электронно-вычислительных и вычислительных машин

Специфические требования: Законченное среднее (полное) общее образование. Пол не регламентируется. Медицинские ограничения регламентированы Перечнем противопоказаний Министерства здравоохранения Российской Федерации.

Квалификационная характеристика профессии "Оператор электронно-вычислительных и вычислительных машин"

Оператор электронно-вычислительных и вычислительных машин должен знать:

- требования по технике безопасности при работе с ПК;
- правила технической эксплуатации и технико-эксплуатационные характеристики вычислительных машин;
- методы контроля работы машин;
- рабочие инструкции;
- разновидности программного и системного обеспечения;
- основные функции и сообщения операционной системы;
- принципы работы со специализированными пакетами программ;
- наиболее распространенное программное обеспечение ПК;
- правила работы и программное обеспечение для работы в сети;
- принципы построения локальных и глобальных вычислительных сетей (в том числе Internet);

- формы обрабатываемой первичной документации;
- формы исходных и выпускаемых документов;
- виды и основные характеристики носителей информации, включая перфокарты и перфоленты, характеристики периферийных устройств, способы подключения периферийных устройств, варианты устранения простейших сбоев;
- основы законодательства;
- основы профессиональной этики;
- запись об использовании машинного времени и замеченных дефектах работы машин в журнал по учету машинного времени;
- руководящие материалы, определяющие последовательность и содержание выполняемых операций технологического процесса;
- правила охраны труда и здоровьесберегающие технологии, электро- и пожарной безопасности, пользование средствами пожаротушения.

Оператор электронно-вычислительных и вычислительных машин должен уметь:

- осуществлять ввод и вывод информации с носителей информации и каналов связи;
- выполнять ввод информации и ее вывод на печатающее устройство;
- вести процесс обработки информации на ПК;
- передавать по каналам связи, полученные на машинах расчетные данные на последующие операции;
- осуществлять внешний контроль принимаемых на обработку документов и регистрацию их в журнале;
- подготавливать документы и технические носители информации для передачи на следующие операции технологического процесса;
- выполнять обработку информации и оформлять результаты выполненных работ в соответствии с инструкциями;
- производить арифметическую обработку первичных документов на вычислительных машинах различного типа с выводом исходных данных и результатов подсчета;
- обрабатывать входящие данные путём суммирования показателей сводок, вычислений по инженерно-конструкторским расчетам;
- выполнять суммирование и таксировку цифровых данных;
- вычислять процентные отношения, операции с константой, возведение в степень, извлечение корня, хранение и накопление чисел и массивов данных;
- проводить сортировку, раскладку, выборку, подборку, объединение массивов на вычислительных машинах по справочным и справочно-группировочным признакам;
- контролировать вычисления, выверять расхождения по первичному документу;
- работать с математическими справочниками и таблицами;
- подготавливать машину к работе;
- определять и устранять сбои в работе аппаратного и программного обеспечения;
- производить установку операционных систем, подключение периферийных устройств, установку антивирусных программ;
- работать с шаблоном;
- вводить текстовую информацию в беглом режиме;
- работать в локальных и глобальных вычислительных сетях (в том числе Internet);
- выполнять правила охраны труда и противопожарной безопасности.

1.5. Количество часов на производственную практику – 396 часов.